Description

METHODS AND SYSTEMS FOR CLINICAL TRIAL DATA GATHERING AND MANAGEMENT

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U. S. Provisional Application Serial No. 60/474,455 Filed May 30, 2003.

BACKGROUND OF INVENTION

[0002] In pharmaceutical development, one critical aspect of the process involves performing clinical trials of a proposed new pharmaceutical or medical device in preparation for regulatory approval. Such clinical trials involve usage of the proposed new pharmaceutical or medical device on a large number of patients and monitoring of results and potential side effects of such usage in each patient. Such clinical trials are done in phases and span a significant period of time. Timely and accurate collection and management of such clinical trial data has presented an on

going problem for the industry.

[0003] In general, even at present, most clinical trial data gathering and management involves substantial manual processing. A clinician (i.e., physician, investigator, medical designee, or other health care personnel) must first determine if a patient is a candidate for a clinical trial and if so complete an enrollment process with the organization managing the trial. (often referred to as the Contract Research Organization or CRO but this could also be a CRO like group at the company or organization sponsoring the research; also known as the sponsor. For purposes of this patent, we use "Data Service Provider" to refer to any organization managing the clinical trial). Once enrolled, a series of visits, treatments and testing is set up for the patient which must be closely monitored and documented. The clinician gathers data associated with examination of the patient at various stages of the clinical trial process. The clinician generally prepares handwritten notes and documents indicating results of the examination. Often the information is provided by filling out a form requesting standardized data regarding the clinical trial. Such information is then forwarded in a secure manner to the Data Service Provider for entry, data validation

and analysis. Typically the papers produced by the clinician are faxed or mailed to the data entry service provider. Such data entry service providers receive clinical trial data from various clinicians and enter the data into a centralized server database for further analysis. Due to the critical nature of the data in regulatory processing, the data is often entered twice and then cross-checked to verify its accuracy with respect to the original handwritten or drawn information. Data so entered and validated in the central server database may then be used to perform required analysis and to produce required regulatory information for submissions to regulatory agencies. Any errors are referred to as Queries and must be resolved with the clinician. Paper based entry systems are subject to many queries as handwriting and terminology may differ among clinicians.

[0004] At all stages of such processes, data security is critical due to the sensitive nature of the information. The information is sensitive with respect to patient confidentiality as well as pharmaceutical industry competition. Paper documents and reports produced by the clinicians' examination must be physically secured as required by regulatory agencies. Paper documents are faxed or mailed to the

service provided as a secure means of communication. An authorized data entry service provider then imposes still further physical and electronic security measures on the data received and entered.

[0005] Although data entry and management automated systems have advanced, the clinical trial data gathering and management industry has been slow to adopt such new technologies. A number of factors may explain reluctance to adopt new technologies. First, the new technologies have not adapted to provide a friendly user interface for a typical clinician. For example, present clinical trial data collection and management systems do not permit a clinician to easily enter handwritten or drawn annotations to an examination report. Still further, the need for high security with respect to the gathered data and the need for auditable verification of the process from the clinician through various intermediates to the final central system database still imposes a significant burden on the clinician. At best, present electronic or web based systems may have moved the data re-keying process into the clinician's office where his/her staff may re-enter the clinician's data from notes taken in the patient exam. This process continues to involve manual steps to transfer data

from the clinician to associated staff people. Maintaining such manual procedures as presently practiced imposes delays and hence cost on the process of clinical trial data gathering and management. These additional costs and delays may ripple into other costs and delays in the phar-maceutical development and regulatory approval process.

[0006] It therefore remains an ongoing problem for the pharma-ceuticals industry to gather and manage clinical trial data in such a manner to assure required security and accuracy while at the same time reducing the need for manual in-tervention and hence improving productivity, speed and accuracy in entry of the data.

SUMMARY OF INVENTION

[0007] The present invention solves the above and other prob-lems, thereby advancing the state of the useful arts, through methods and associated structures for more fully automating clinical data gathering and management pro-cesses. Features and aspects hereof provide for secure data entry and storage in all electronic form directly from the examining clinician. In one specific aspect hereof, a remote computing device (such as a tablet PC, laptop computer or other handheld remote computing device) in the hands of the examining clinician permits direct, elec-

tronic data entry from the clinician to the clinical data management systems. Such a remote computing device may permit entry of data both as "fill in the blanks" electronic forms as well as digitized images of handwritten notes or hand drawn figures. Form data entered at such a remote computing device may be locally validated by processing power local to the remote computing device. Handwritten notes and figures may also be saved as digitized images to be forwarded to the central server database.

[0008] In another aspect hereof, electronic data entered by a clinician on the remote computing device maybe securely stored locally during periods of time that the remote computing device is without communications to a central server. When the remote computing device again establishes communication to the central server, data may be transmitted thereto immediately following local validation. When the remote computing device is temporarily without communication capabilities to the central server, security features hereof permit the data to be locally validated and stored secured from unauthorized access until such time as communications with the central server is again established. These and other aspects hereof also permit wire-

less communications to be utilized between the remote computing device and the centralized data management server, although wireless communication capability is not a requirement. By allowing the clinician an interface that simplifies direct data entry, intermediate steps requiring the manual re-keying of data by a data entry service provider may be eliminated thus improving both accuracy of the gathered data and speed in the gathering of such data.

BRIEF DESCRIPTION OF DRAWINGS

[0009] Figure 1 is a block diagram of an exemplary system in which features and aspects hereof may be advantageously applied.

[0010] Figure 2 is a flowchart describing a method for clinical trial data collection at a remote computing device.

[0011] Figure 3 is a flowchart describing a method for receiving and archiving clinical trial data within a central server.

[0012] Figure 4 is a flowchart describing a method for reporting clinical trial data archived in a central server.

DETAILED DESCRIPTION

[0013] Figure 1 is a block diagram of a system 100 embodying features and aspects hereof. Remote computing device

108 interacts with a clinician examining the patient participating in a clinical trial study. The clinician may enter data on remote computing device 108 either as handwritten or hand drawn images or as data entered into fields of a form, or both. Such a form may correspond to standardized information required in the clinical trial study and may therefore prompt the clinician to respond with the requested information. Image data entry element 114 may receive such handwritten or hand drawn information and digitizes such information to be stored in association with form data required in the clinical trial study. Form data presentation, entry and the validation element 116 is operable to present form data to a clinician, to receive clinician responses for the requested information, and to validate the clinicians entered responses. In one aspect hereof, element 116 may present the user with a form to be filled in accordance with XML format definitions (i.e., an XML schema). Such an XML schema may define, among other things, the format for presentation of information to the clinician as well as fields for entry of clinician responses. Still further, an XML schema may define validation criteria (i.e., data edits). These validation criteria may be applied locally by operation of the remote computing

device 108 to verify the entered data in accord with the XML schema. Further validation of such entered information may also be provided by the central server as discussed further herein below.

[0014] Remote computing device 108 may also include a secure local storage medium 112 in which clinical trial data entered it by the clinician may be temporarily stored in a secure manner. As noted above, regulatory requirements for such clinical trial data may include security requirements to prevent unauthorized access to private medical information associated with the clinical trial patient. Still further, corporate security measures imposed within the pharmaceutical development industry may require still stricter security measures to further preclude unauthorized access to the gathered clinical trial data. Local secure storage element 112 may be implemented as any of several well known storage media including, for example, nonvolatile semiconductor memory components (i.e., PC card memory modules or flash memory modules), magnetic disk or tape storage media, optical disk or tape storage media, etc. Security for such a storage media may be provided in a number of forms depending on regulatory and corporate security requirements. In one aspect

hereof, security may be provided as client certificates providing digital encryption techniques using public and/or private key encryption. In one example, such an encryption key may be generated as a function of a supplied user ID and password. Numerous other digital encryption techniques will be readily apparent to those of ordinary skill in the art. All such encryption techniques may be useful for securing the storage of sensitive data in local secure storage element 112.

[0015] Remote computing device 108 may include communication link 110 adapted for communicating with an associated central server system (i.e., central server 102 of system 100). Communication link 110 may provide, for example, network communication features to couple the remote computing device 108 to a central server using any of numerous well known computer networking techniques. As required in a particular application, communication link 110 may also provide encryption or other security techniques to secure data transmission between the remote computing device 108 and an associated server from unauthorized interception. In one aspect hereof, communication link 110 provides a wireless networking communication feature for coupling the remote comput-

ing device to an associated central server 102 without the need for a tethered connection that may restrict less convenient. Such a wireless communication technique further simplifies use of the remote computing device 108 for a non-technical clinician desiring ease of use. Wireless networking communication is not a requirement since data collected offline may be readily and securely posted to the centralized server whenever a hard wired connection is available. Numerous other computer networking connections may be provided by communications link 110 to couple remote computing device 108 to associated central server 102 as required in a particular application.

[0016] Remote computing device 108 may be implemented as any remote computer system useful for a particular application including, for example, handheld devices such as laptop or notebook computers, personal digital assistants (PDAs) and tablet PC systems. Features and aspects of the remote computing device 108 may also be provided by less mobile (i.e., desktop) but with some loss of flexibility in the lack of mobility. Ease of use as reflected by the mobility of a handheld remote device is one desirable, though not required, aspect hereof. In one particular aspect hereof, so-called tablet PC system may be used for

remote computing device 108. Such a tablet PC provides desired features for local validation and entry of form data, for secure storage of such entered data, and for input of digitized images of handwritten or hand drawn ancillary information from the clinician.

[0017] Central server 102 of system 100 generally provides centralized storage and archiving of clinical trial data gathered from one or more remote computing devices 108. Numerous clinicians, each using a remote computing device 108, may enter clinical trial data during examination procedures of each clinic hr study patient. As noted above, such clinical trial data may be initially stored locally within the remote computing device and, when conductivity permits, forwarded at a later time to the central server 102. Central server 102 may therefore include a communication link 106 similar to the communication link 110 described above with respect to remote computing device 108. Communication link 106 may provide network connectivity to one or more remote computing devices 108 as discussed above. In one aspect hereof, communication link 106 provides a wireless network communication link to one or more remote computing devices 108. As further noted above, such wireless communication

links enable additional mobility and flexibility for clinicians utilizing remote computing devices to enter data during clinical trial patient examinations.

[0018] Central server 102 may further include XML reformatting element 107 to provide desired reformatting of clinical trial data stored by central server 102. Such reformatting may include generation of desired reports useful in the regulatory process as well as other administrative reporting to provide desired statistical summaries and analysis of gathered clinical trial data. Central secure storage 104 may be associated with a central server 102 as a central repository of gathered clinical trial data. Central secure storage 104 may be coupled to central server 102 either locally or remotely via path 156.

[0019] As noted above, although significant validation and verification of entered clinical trial data may be provided by remote computing device 108, central server 102 may include within XML data reformatting element 107 the capability of further verification and validation of data provided by an associated remote computing device 108. Where such an additional validation or verification indicates a problem with provided clinical trial data, the data may be returned to the remote computing device with an

appropriate error or status indicator to permit correction and reentry of the provided clinical trial data.

[0020] As a above with respect to remote computing device 108, central server 102 may apply digital encryption techniques to assure security of any communications with remote computing devices 108 as well as to assure security of clinical trial data stored within central secure storage 104. As above, client/server certificates generated based upon user ID's and/or passwords may be utilized to provide such encryption security. Numerous other well known forms of encryption and security may be applied to assure the desired level of security for communications with remote computing devices and for storage of private clinical trial data.

[0021] Central server 102 may be coupled via path 152 to a network communication medium 150. In like manner, remote computing device 108 may be coupled via path 154 to communication medium 155. As discussed above, central server 102 may be coupled thereto through communication link 106 while remote computing device 108 may be coupled with thereto via communication link 110. Communication medium 150 may be any appropriate medium for transmission of clinical trial data between one or more

remote computing devices 108 and a central server 102. Such communication media may be, for example, Ethernet, token ring, Fibre Channel (or other optical communication media), as well as wireless communication features utilizing RE or other frequencies of the electromagnetic radiation spectrum. The associated communication link (i.e., 106 and 110) and the communication medium 150 may preferably provide any desired level of security through data encryption or other well known encryption and security techniques.

[0022] Figures 2 through 4 are flowcharts describing processes operable within a system such as described above with respect to Fig. 1. In particular, Fig. 2 describes a process operable within a remote computing device including, for example, PDAs, laptop or notebook computers, tablet PC systems and the like. Element 200 is first operable to receive or otherwise retrieve an XML form designed for clinical trial data entry. The XML form may be previously received from an associated central server system or other repository of XML forms useful for clinical trial data entry. Alternatively, the XML form may be locally stored (i.e., cached) within the remote computing device. Element 202 then presents the XML form on a display associated with

the remote computing device. Element 204 next awaits receipt of input from the clinician user of the remote computing device indicating entry of information in some field(s) of the displayed XML form.

[0023] If the received clinician input is manually entered information (i.e., handwritten or hand drawn annotations), as determined by element 206, processing continues with element 208 to digitize such manually entered information followed by element 210 to temporarily store the digitized information in the local secure store. Digitizing of such manually entered information may consist of scanning paper documents using a scanner feature associated with the remote computing device or may comprise direct receipt of digitized information as sketched into an electronic digitizing tablet associated with the remote computing device. As noted elsewhere herein, in one aspect of the invention, a tablet PC having such a digitizing surface integrated within may be used for entry of such manual information. Following digitized entry of the information and temporary storage of the digitized image, processing continues with element 204 to await further clinician user input.

[0024] If element 206 determines that the received clinician input

is not manually entered information but rather entry of data in fields of the form presently displayed, element 212 is next operable to perform validation functions on the data field just entered. Such a validation may be in accordance with information imbedded in the XML schema of the presented form. So called "data edits" may be defined within an XML schema to indicate test criteria which may be applied to the corresponding data entry field to determine whether the entered data complies with expected values or ranges. Numerous types of data edits may be associated with an XML schema as well known to those of ordinary skill in the art. Numerous other validation processes may also be applied where XML schemas are not utilized to define the desired, expected data values and ranges.

[0025] If the validation process of element 212 indicates that the data is not valid as determined by element 214, element 216 is next operable to permit the clinician user to correct the erroneous data entry. If the clinician enters corrected information, processing returns to element 212 to again verify correctness of the newly corrected data entry. If the clinician chooses not to enter corrected data as determined by element 216, element 218 allows the clinician to

enter an annotation explaining the discrepancy in the entered data field. If the clinician enters such an annotation explaining the discrepancy, element 220 is next operable to annotate the entered data in temporary storage with the provided explanation regarding the validation discrepancy. If no such annotation is entered by the clinician user as determined by element 218, element 222 is operable to annotate the entered data field as an unresolved discrepancy. Such unresolved discrepancies may be resolved at a later time in the clinical trial study. In either case, processing continues with element 224 as discussed herein below.

[0026] Once valid data has been entered as determined by element 214, or appropriate annotations are provided by elements 220 or 222, element 224 is next operable to determine whether the clinician has indicated that the data fields entered in the form are completed and therefore ready for submission to further processing. If the form is not yet complete, processing continues at element 204 to await further input from the clinician. If element 224 determines that the clinician has indicated completion of the form by requesting submission thereof, element 226 is next operable to generate a client certificate to secure the

submitted data from unauthorized access. As noted above, numerous security techniques and structures may be implied to provide the desired security from unauthorized access. Digital data encryption utilizing public or private keys or so called client certificates are but exemplary of such security measures.

[0027] Element 228 is then operable to store the entered form data and any associated digitized images data in a secure local store associated with the remote computing device. As noted above, the secure local store is secured from unauthorized access through the client certificate or other security and encryption techniques as discussed above. The data so stored may be forwarded to the central server for permanent storage when communication capabilities allow such transmission. Element 230 is therefore operable to determine whether the central server is presently connected to the remote computing device. If not, processing of the method completes with the entered form data and associated digitized images data stored in the secure local store of the remote computing device. The central server may be temporarily inaccessible due to a failure of the communication link or communication medium or, as in the case of wireless communications,

temporarily out of range. If element 230 determines that the central server is presently connected or if the connection is later restored (i.e., a wireless connection brought it back in range), element 232 is next operable to forward the locally stored data to the central server. Central server may provide a permanent archive of the clinical trial data as well as security features to preclude unauthorized access thereto. Since the central server may provide such a permanent archival storage, the remote computing device may remove its locally stored copy of the forwarded clinical trial data. Well known communication techniques and protocols may be employed to verify proper receipt of the forwarded clinical trial data such that it may be erased from the remote computing device upon verification of proper receipt. In addition, features of the central server may provide further validation of the forwarded clinical trial data. If an error is detected from such additional validation, the remote computing device may be so notified to permit corrective action by the clinician at the remote computing device. Alternatively, such corrective actions may be provided by users of the central server.

[0028] Those of ordinary skill in the art will recognize a variety of equivalent processes and steps to implement features and

aspects hereof. The process of Fig. 2 is therefore intended merely as exemplary of one such process for providing features and aspects hereof.

[0029] Figs. 3 and 4 describe processes operable on a central server that provides centralized, permanent archive storage of clinical trial data as well as reporting and analysis tools therefore. In particular, Fig. 3 represents a process for receiving validated data from a remote computing device for persistent storage in the central server. Element 300 is first operable to receive such validated data from an associated remote computing device. Element 302 is next operable to further validate the received data. Although validation may be performed within the remote computing device as discussed above, further validation may be provided by the central server in view of its centralized store of other clinical trial data. For example, validation within the central server may include processing to detect duplicate entries for a particular patient or other anomalous or unauthorized data entry requests. If element 304 determines that the received data passes such a further validation, element 306 is then operable to add the newly received data to the secure central database of the central server. If element 304 determines that the re-

ceived data fails to pass the additional validation, element 308 is operable to return an appropriate error indication to the remote computing device to permit further processing by the clinician. As noted above, such corrective actions may also be provided by users of the central system to avoid returning the invalid data to the clinician.

[0030] Fig. 4 is a flowchart describing a process operable within the central server for generating requested reports or analysis based on information saved in the secure central store associated with the central server. Element 400 awaits a user request for generation of an identified report or analysis. Element 402 then retrieves all appropriate data from the secured central database required to generate the identified report. Appropriate security measures may be employed to preclude unauthorized access by the requesting user. Element 404 then reformats the retrieved data according to the desired report requirements.

[0031] Data stored in and retrieved from the central database may be stored and retrieved as XML data messages allowing simple yet flexible reformatting capabilities. Element 406 transmits the reformatted report information to the requesting user or an appropriate regulatory agency as

appropriate to the particular application.

[0032] Those of ordinary skill in the art will recognize a wide variety of similar processes operable within a central server to receive and store data from a remote computing device and to generate requested analysis reports therefrom. Figs. 3 and 4 therefore represent merely exemplary processes for achieving desired features and aspects hereof.

[0033] While the invention has been illustrated and described in the drawings and foregoing description, such illustration and description is to be considered as exemplary and not restrictive in character. One embodiment of the invention and minor variants thereof have been shown and described. Protection is desired for all changes and modifications that come within the spirit of the invention. Those skilled in the art will appreciate variations of the above-described embodiments that fall within the scope of the invention. As a result, the invention is not limited to the specific examples and illustrations discussed above, but only by the following claims and their equivalents.